

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA)	Case No. 1:19-CR-367
)	
v.)	The Hon. Anthony J. Trenga
)	
SEAN MICHAEL MCLAUGHLIN,)	Bench Trial: August 20, 2020
)	
Defendant.)	
_____)	

UNITED STATES' REBUTTAL CLOSING STATEMENT

The defendant's closing statement appears to address a different case with a different set of facts. So what is this case? This is a case where the defendant provided a detailed confession to committing the serious crimes of receipt and possession of child pornography.¹ His confession provided a starting point for law enforcement on *how* to conduct the forensic examination of his computer. This forensic examination corroborated the defendant's admissions in both large and small ways. Both the defendant's admissions and the forensics prove that the defendant was a frequent and long-time consumer of child pornography, which he obtained using the Shareaza program.

At bottom then this is a straightforward case. There are no unanswered questions. The evidence proves that the defendant did exactly what he said he did: he received and possessed child pornography over a long period. Further, if the defendant's statements and the forensics in

¹ The term "child pornography" will be used in this Rebuttal Closing Statement to refer to visual depictions of minors engaged in sexually explicit conduct, as those terms are defined in 18 U.S.C. § 2256.

this case are not enough to convict the defendant, then it is difficult to imagine what evidence could ever be enough. For this reason, the United States asks this Court to return the only verdict supported by the evidence, and that is a verdict of guilty on both counts.²

I. The Defendant Provided a Detailed Confession to the Crimes of Receipt and Possession of Child Pornography

The defendant has failed to come to grips with the fact that he confessed to both receiving and possessing child pornography. And, it is clear the defendant is avoiding dealing with his statement because he provided a comprehensive confession. Rather, than address his statements, the defendant has rather fantastically argued that his admissions provide nothing more than “propensity evidence.” Defendant’s Closing Arguments and Renewed Motion for Judgement of Acquittal (“Def Closing”) at pg. 7. Of course, just the opposite it is true. The defendant’s admissions are a roadmap to how and why he committed the crimes of receipt and possession of child pornography.

It is undisputed that the defendant consented to a voluntary interview with Special Agent Raymond Abruzzese. Because this interview is recorded, there can also be no dispute over what the defendant admitted. The defendant is fond of quoting from the expert’s testimony; so, for the sake of clarity, the United States will highlight some of the defendant’s key admissions.

First, the defendant admitted to using the internet to download many videos containing child pornography. For instance, the defendant admitted to downloading at least 50 videos of child pornography — some of them on multiple occasions — in the year preceding his interview

² The defendant has also renewed his Motion for Judgment of Acquittal. The United States submits that the evidence proves beyond a reasonable doubt that the defendant is guilty of both receiving and possessing child pornography. Separately, if the evidence is viewed in a light most favorable to the government then the defendant’s confession coupled with his search terms alone is more than enough evidence for a rational trier of fact to find the defendant guilty of attempted receipt and possession of child pornography.

on January 25, 2018. He also admitted that he deleted the videos containing child pornography after he viewed him.

SPECIAL AGENT ABRUZZESE: Yeah.

If you had to put a number on it, how many videos do you think that you've downloaded in your --

MR. McLAUGHLIN: Lifetime?

SPECIAL AGENT ABRUZZESE: Well let's just go the last year. How many -- I'm talking about child pornography. I'm not talking about videos, like, you know --

MR. McLAUGHLIN: (Indiscernible) I'm not sure.

SPECIAL AGENT ABRUZZESE: Okay. Well --

MR. McLAUGHLIN: I don't know, like probably over 50. Some of them are the same videos I download, then I delete -- delete the program. Then put the program back on and I download the same videos. At least 50 is a safe bet. Probably more.

See Exhibit 1-2 at pgs. 51–52.

In this passage alone, the defendant admitted to knowingly receiving and possessing child pornography.

Second, in the below passage, the defendant detailed when he began downloading child pornography. He also detailed the search terms that he used in Shareaza to obtain child pornography.

SPECIAL AGENT TORRES: How did you know how to look for this? How did you find it?

MR. McLAUGHLIN: So when I, when I first started doing it when I was young, I don't remember if I just searched for like 13-year old, 14-year old boys or like, 13-year old gay or whatever. But there's code words you start seeing on videos, "P one-on-one" --

SPECIAL AGENT ABRUZZESE: "P one-on-one?"

MR. McLAUGHLIN: "RBV" -- yeah.

SPECIAL AGENT TORRES: What does that mean?

MR. McLAUGHLIN: I have no idea. I think -- RBV is probably like, something boy video. Disc cam. I mean, there's, there's a couple of different ones.

“Yahmad.” I don't even know what that means.

SPECIAL AGENT TORRES: So you started seeing those on certain videos then you started searching for the same things, hoping -- okay.

MR. McLAUGHLIN: Yeah.

SPECIAL AGENT ABRUZZESE: And that's how you look at -- like, on Shareaza or eMule? You'll put in those search terms or your specific videos?

MR. McLAUGHLIN: Sometimes specific videos. Sometimes just the search terms. I mean, not like, specific videos, just -- they have like, a lot of times, fairly long titles.

SPECIAL AGENT ABRUZZESE: Right.

MR. McLAUGHLIN: But like, if you know what you're looking for, like say, 13-year old whatever, you just type in like, “P one-on-one, 13-year old,” and it'll pull up like a list of similar ones.

Id. at pgs. 52–53.

Third, in the following passages, the defendant made clear he searched for videos containing young children.

SPECIAL AGENT TORRES: I know you started with 13s. Did you find yourself looking for younger?

MR. McLAUGHLIN: Generally, it was between like, 16 and like, 7, 8, was my usual range.

SPECIAL AGENT TORRES: Mm-hmm.

MR. McLAUGHLIN: Usually more towards like the 12-ish range.

SPECIAL AGENT TORRES: Okay.

SPECIAL AGENT ABRUZZESE: Because the stuff that I've downloaded from you --

MR. McLAUGHLIN: Was younger.

SPECIAL AGENT ABRUZZESE: -- was younger than that. It was the five, six, seven-year-old range. So -- but you're saying typically you would target older?

MR. McLAUGHLIN: Usually, yeah.

SPECIAL AGENT ABRUZZESE: Okay. No infant?

MR. McLAUGHLIN: No.

SPECIAL AGENT ABRUZZESE: Okay.

MR. McLAUGHLIN: Not on purpose though.

SPECIAL AGENT ABRUZZESE: But have you downloaded infant porn?

MR. McLAUGHLIN: Maybe by accident. Sometimes they'll have videos that are labeled one thing and they're something different.

SPECIAL AGENT TORRES: What did you think of those?

MR. McLAUGHLIN: I -- I don't like any of it.

SPECIAL AGENT TORRES: Mm-hmm.

MR. McLAUGHLIN: It wasn't as -- it wasn't like, arousing.

SPECIAL AGENT TORRES: Mm-hmm.

MR. McLAUGHLIN: Whereas like, I, I know I don't like the other stuff, either, but it was arousing.

Id. at pgs. 53–54.

Moreover, the defendant again admitted that he downloaded child pornography because he found it arousing to watch. He also admitted to storing child pornography on flash drives.

SPECIAL AGENT ABRUZZESE: Okay. But the videos that you download, I mean, I'm assuming that you'd watch it like you -- someone else would watch adult porn, you do it for -- you know, to masturbate.

MR. McLAUGHLIN: Yeah. And then a lot of times, right afterwards, I delete the whole thing. I had -- I've put them on flash drives before where I've actually broken the flash drives, just trying to get -- just -- I want to stop.

Id. at pg. 15.

Finally, the defendant made clear that he searched for child pornography using his Asus tablet and that neither his mother nor his fiancé, Mr. Hodges, were involved.

SPECIAL AGENT ABRUZZESE: All right. And the last time you downloaded anything was when you -- what, November you said?

MR. McLAUGHLIN: That probably sounds right. It was sometime after I moved in here.

SPECIAL AGENT ABRUZZESE: Okay. And what program were you using?

MR. McLAUGHLIN: Probably Shareaza or BitTorrent.

SPECIAL AGENT ABRUZZESE: Okay. I know -- and I hate to ask the same question over and over again. But I know you said you were using your tablet and you used the laptop.

MR. McLAUGHLIN: I don't know if I used that one.

SPECIAL AGENT ABRUZZESE: Okay.

MR. McLAUGHLIN: I may have --

SPECIAL AGENT ABRUZZESE: Used a --

MR. McLAUGHLIN: -- at my mom's, but yeah.

SPECIAL AGENT ABRUZZESE: So mostly the tablet or --

MR. McLAUGHLIN: Mostly the tablet, yeah.

Id. at pgs. 18–19.

SPECIAL AGENT ABRUZZESE: Okay. Is this exclusively yours or --

MR. McLAUGHLIN: That's exclusively mine.

SPECIAL AGENT ABRUZZESE: Okay. And that's the -- I mean, sorry, that's the tablet.

MR. McLAUGHLIN: Yeah. James [Mr. Hodges] doesn't know anything about this. My mom, she may have caught me when I was younger, but she didn't know what I was doing.

Id. at pg. 34.

The statements highlighted above are just a few of the defendant's admissions. Even assuming that admissions can be characterized as mere "propensity evidence," the defendant clearly provided a roadmap to how and why he received and possessed child pornography. The defendant admitted to using Shareaza and other internet-based programs to search for and download child pornography. He admitted to viewing child pornography because he found it sexually arousing. He provided some of the search terms he used to obtain child pornography, including "p101," "RBV," and "Yamad." He also admitted that he used his Asus tablet, a laptop, and flash drives. Finally, the defendant admitted that he deleted the child pornography after

viewing it, only to begin the cycle all over again by repeatedly searching for, downloading, and viewing many of the same child pornography videos.

II. The United States Fully Corroborated the Defendant's Confession

The defendant argues that the United States' case rests on the assumption that a crime has been committed and then consists of showing how each piece of circumstantial evidence can be explained in a way consistent with this assumption. Def Closing at pg. 4. The defendant's argument is built on a house of cards because he once again ignores that he confessed to committing the crimes of receipt and possession of child pornography.

This is a case where the defendant provided a thorough and detailed confession. Under the law, the United States must introduce independent evidence that corroborates the defendant's confession. *See, e.g., United States v. Oppen*, 348 U.S. 84, 93 (1954) (holding the government must "introduce substantial independent evidence which would tend to establish the trustworthiness of the [defendant's] statement." But this "corroborative evidence need not be sufficient, independent of the [defendant's incriminatory] statements, to establish the *corpus delicti*."); *Wong Sun v. United States*, 371 U.S. 471, 489 (1963) (noting "extrinsic proof [i]s sufficient which merely fortifies the truth of the confession, without independently establishing the crime charged" (internal quotation marks omitted)). *United States v. Abu Ali*, 528 F.3d 210, 235–36 (4th Cir. 2008) (holding the United States introduced "significant independent circumstantial evidence tending to establish the trustworthiness of [the defendant's confession]"); *cf. United States v. Rodriguez-Soriano*, 931 F.3d 281 (4th Cir. 2019) (applying the legal standard from *Abu Ali*, but holding the United States failed to introduce independent evidence that a crime was committed because "all of the evidence the government claim[ed] corroborate[d] [the defendant's] confession [arose] from his own statements to law enforcement"). This independent evidence must sufficiently support the essential facts admitted

to justify an inference that the defendant was telling the truth to Special Agent Abruzzese. The United States has done this and more when it introduced significant forensic evidence, which corroborates the defendant's admissions in both big and small ways.

A. Extensive Forensic Evidence Corroborates the Defendant's Admissions that He Received and Possessed Child Pornography

As thoroughly briefed in the United States' Closing Statement, the United States introduced a mountain of evidence corroborating every aspect of the defendant's confession. This evidence included Shareaza searches and child pornography in folders associated with Shareaza.³ The evidence also included jumplists, LNK files, and MRU entries, showing that the defendant viewed child pornography on both the tablet and the laptop, along with thumbnails of some images showing that child pornography had both been on the tablet and had been previewed. Finally, the recycle bin evidence included numerous titles indicative of child pornography. Below, we detail in painstaking detail how specific pieces of evidence corroborate the defendant's statements.⁴

When the defendant said that he downloaded "like probably over 50" child pornography videos in the previous year and clarified that "[a]t least 50 is a safe bet" but it was "[p]robably more," he was right. If the Court looks at GE 6-4B—the tablet jumplist entries showing child pornography viewing—72 files with titles indicative of child pornography were created in the

³ The defendant incorrectly states that "[t]he only complete files of child pornography recovered . . . were in the recycle bin." Def Closing at pg. 11. This ignores the 35 files of child pornography found in the Shareaza\Collections folder, which is the folder under the Seanm_000 user profile where "collections" of Shareaza files went and that was divided into the folders "BoyFuck Magazine" and "Men fuck preteen boys with picture preview." GEs 6-3B, 6-11A–D.

⁴ The defendant said he mostly used the tablet to receive and view child pornography. The forensic evidence corroborates this admission; and, accordingly, the tablet will be the focus of the discussion here. The evidence tied to the laptop was thoroughly addressed in the United States' Closing Statement.

year before the defendant's statement, all in the "Downloads" folder where Shareaza placed files. *See* Attachment A (GE 6-4B with the files created in the year preceding the defendant's statement "checked" for ease of review). Similarly, when the defendant said he downloaded the same videos multiple times, this is easily observed from the summary exhibits. *See* GEs 9-3 (two copies of file), 9-4 (three copies), 9-5 (two copies), 9-6 (three copies), 9-7 (three copies), 9-8 (three copies), 9-9 (three copies), 9-10 (two copies), 9-11 (four copies), 9-14 (four copies), 9-15 (two copies), and 9-16 (three copies).⁵ The defendant also said that he stored child pornography on flash drives, and the forensic evidence corroborates this, showing that he viewed child pornography files from removable drives. *See* GEs 6-4C & 6-5C.

The defendant also explained some of the search terms he used in Shareaza to find child pornography, including "p101," "p101, 13 year old" "RBV," and "yamad." GE 1-2 at pgs. 52–53. And, sure enough, the tablet reflects that he used exactly those search terms. *See* GE 6-3C record 13 ("p101 . . ."), record 58 ("p101"), record 77 ("p101 kdv"), record 81 ("p101 kdv boy 10yo"), record 86 ("p101 boy 10yo man . . ."), record 100 ("p101 brotherlove"), record 189 ("rbv pjk yamad"), record 195 ("boy pjk rbv . . ."), and record 202 ("p101 . . .").⁶ The Court need not speculate whether these search terms were actually effective, because the Court can see in GE 6-3D that the terms produced files with names indicative of child pornography. Moreover, the search terms captured in GEs 6-3C and 6-3D are the type of significant independent

⁵ Law enforcement downloaded the final three files in this case from a Shareaza user on an IP address tied to where the Defendant was living with his mother. *See* GEs 2-2, 4-1, 4-9A,B, 4-3A,B, and 4-4A,B

⁶ This stands in stark contrast to the searches that the defendant points to from *Dillingham*. Here, instead, the defendant confessed to using multiple, sophisticated search terms to find child pornography on peer-to-peer programs and the forensics show those *exact* search terms being used in the *exact* peer-to-peer program he said he used. Further, there can be no question that the defendant was doing this from 2014 to 2018, because the defendant admitted to downloading over 50 files of child pornography in the year preceding his interview on January 25, 2018 alone.

circumstantial evidence that establishes the trustworthiness of the defendant's confession. *See Abu Ali*, 528 F.3d at 236. These terms also prove beyond a reasonable doubt that the defendant attempted to receive child pornography every time he used "p101" and the other search terms he identified.

Inexplicably, the defendant again tries to link this case to the Court's previous decision in *Dillingham*—a markedly different case—by arguing that the government must prove the defendant received the "Known Images," a phrase the government used in *Dillingham*. Yet, this terminology shows just one of the many differences between these cases, because the government in its opening statement, closing argument, and opposition to the motion for acquittal in *Dillingham* relied only on what they called the "Known Images" as the basis of the charges. Further, at a hearing on the motion for acquittal, the government also conceded that "that the Defendant was charged only with receiving and distributing the Known Images." *United States v. Dillingham*, 1:17-cr-184-AJT, ECF No. 84, pg. 7. The United States here has made no such concession, nor has the government ever limited itself to a specific collection of images.

In addition to the mountain of attribution evidence introduced at trial and outlined in the United States' Closing Statement, there is much more. Perhaps the best illustration of this is one of the defendant's last periods of engaging in his cycle of searching for, downloading, viewing, and deleting child pornography before law enforcement caught him. More specifically, the period from October 7 to 21, 2017.⁷ *See* Attachment B.⁸ On October 7, 2017, program files

⁷ Of note, this also tracks the defendant's admission that the last time he downloaded child pornography was "around November." GE 1-2 at pg. 18.

⁸ As with the demonstratives used in the United States' Closing Statement, this attachment is a demonstrative created by combining admitted exhibits and sorting by the "target file created

associated with Shareaza were created. One hour later, a file with a title indicative of child pornography was created in the defendant's "Downloads" folder.⁹ Files with titles indicative of child pornography continued to be created in the "Downloads" folder into the following day, including the files addressed in GEs 9-4, 9-8, and 9-11. After a one-day break, more files with titles indicative of child pornography were created on October 10, 2017, including the files in GEs 9-6, 9-7, and 9-9. After this download binge ended, a deletion period began, including all of the files in the government's exhibits that had been created in the previous three days. The next day the cycle began again, when the files in GEs 9-1 and 9-10 were created in the "Downloads" folder and the files in GEs 9-4, 9-6, 9-7, 9-8, 9-9, 9-10, 9-11, and 9-14 were deleted. After another one-day break, the cycle began again on October 13, 2017, when the file in GE 9-3 was created and the files in GEs 9-7 and 9-8 were deleted. The following day, the files in GEs 9-1, 9-3, 9-4, 9-6, 9-9, 9-10, 9-11, and 9-14 were deleted. After another brief hiatus, a file with a title indicative of child pornography was created in the "Downloads" folder on October 17, 2017. Three days later, a file titled "Certificate for McLaughlin, Sean" was created.¹⁰ Then the child pornography cycle began again, when, on the following day, numerous files with titles indicative of child pornography were created in the "Downloads" folder. For each of these entries, spanning this entire demonstrative exhibit, it bears repeating that the creation date is only available in these records once a file has been accessed.

date/time" and, where applicable, the "deleted date/time." The demonstratives only include the columns that the forensic expert explained the significance of, and only include entries that contain file or folder information.

⁹ As the Court will recall from trial and previous filings, the "Downloads" folder, although not exclusive to Shareaza, is where the Shareaza program placed completed downloads.

¹⁰ Notably, across all the evidence of files being viewed and deleted that was introduced at trial, there are no entries associated with Mr. Hodges in October 2017, which is when this conduct occurred; only, the entry associated with Sean McLaughlin.

Thus, the October activity on the tablet began with the creation of Shareaza program files, then a repetitive cycle of creation and deletion of child pornography, which was viewed in the interim, then a file associated with the defendant was created, followed again by the creation of additional child pornography. This fully corroborates the defendant's admission that he engaged in a cycle of downloading Shareaza, and then searching for, downloading, viewing, and deleting child pornography.

B. The Defendant has Thoroughly Misrepresented the Forensic Expert's Testimony

In an attempt to deflect from the mountain of forensic evidence corroborating his confession, the defendant's closing statement chooses to misrepresent the forensic expert's testimony. The United States will first respond here to the defendant's flawed challenges to the expert's reliability. The United will then respond to four specific instances where the defendant misconstrues the record.

As an initial matter, defense counsel had an opportunity to *voir dire* the expert prior to her certification as an expert, but did not. Indeed, the defendant raised no objection to her certification as an expert in computer forensics either before or after her testimony.¹¹ The

¹¹ The defendant now untimely claims that, based on her credentials known before and during trial and her testimony, her testimony is inadmissible as expert testimony. The appropriate standard for admissibility is met here. For expert testimony to be admissible it must meet four requirements: (1) that the technical or specialized knowledge will assist the factfinder in understanding the evidence, (2) that it is based on sufficient facts or data, (3) that it is the product of reliable principles and methods, and (4) that the expert reliably applied the facts to the case. *See* Fed R. Evid. 702. Furthermore, "the trial court's role as a gatekeeper is not intended to serve as a replacement for the adversary system," and consequently, "the rejection of expert testimony is the exception rather than the rule." Fed. R. Evid. 702 advisory committee's note to 2000 amendment. Here, the forensic expert has attended numerous trainings in computer forensics and has multiple certifications in using computer forensic tools, at least one of which she testified required passing a proficiency test to obtain. Tr. 6:21–5; GE 5-1. She has examined hundreds of electronic devices and continues to receive continuing education in the field. *Id.* The defendant does not identify any particular aspect of Rule 702 in which her testimony is deficient, thus, even setting aside the untimely nature of the challenge, it should be denied.

defendant has not challenged the reliability of the multiple tools she used or the application of those tools. Instead, the defendant primarily relies on a few instances where the expert testified to what “typically” happens on computers. Rather than undermining her credibility, this shows that the expert was not providing overbroad conclusions unsupported by the facts or tools. If the defendant believed these explanations were incorrect or that an atypical possibility was relevant then he was free to cross-examine the expert on those points, but he did not. Instead, the defendant now seeks to have the forensic expert recite that her statements are “to a reasonable degree of certainty.” Because the test for reliability of expert opinions is “flexible” and judges are granted broad latitude in determining reliability, no such talismanic recitation is necessary. *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 141 (1999). Yet, what the defendant does not highlight is that the one time he choose to clarify a statement in which the expert said her testimony was “[f]rom [her] understanding,” and he asked whether this was “to a reasonable degree of certainty,” her immediate and unqualified response was “yes.” Tr. 94:5–18.

As previously addressed in the United States’ Closing Statement, the defendant misconstrues the testimony on whether the laptop was password protected. It was password protected. As the forensic expert explained, the way she accessed the laptop in order to conduct her examination—and thus in order to create GE 7-2—did not require her to enter a password. Tr. 124:12–16. However, when a user “just open[s] up the computer and log[s] in, then [it] would require a password.” Tr. 124:16–18.

The defendant next attempts to create a contradiction where none exists with respect to the forensic expert’s testimony on the searches.dat and ntuser.dat database files maintained by the Shareaza program. On cross-examination, the forensic expert testified that there are two locations where Shareaza logs “when a user enters a keyword search:” “[t]he searches.dat within

the Shareaza folder” and the ntuser.dat under “Shareaza/searches/search” folder. Tr. 97:13–20. Defense counsel asked, and she agreed, “[y]ou can transfer those data files manually from another drive to the destination on the C drive.” Tr. 98:4–10. He went on to ask whether “the user can manually access those destinations, the user can manually place files, including data files, into any of those subfolders,” which the expert testified they could. Tr. 101:22–102:4. On redirect, when asked about the amount of folders a user would have to copy data into for fabricated data to match what she found, the forensic expert explained that “folders that stored under the ntuser.dat where the keyword searches were found, that’s in a database. And unless a user has like third-party software and knows how to export those files out, they can’t access those folders. It’s not readable.” Tr. 139:18–140: 10. All of these answers are consistent. It is *possible* that a user can copy a database file into the Shareaza folders, access the database files, and read the database files. That does not mean that just anyone can do it or that it can be done without special tools or knowledge. The defendant stating that the expert testified that “.dat files can *easily* be transferred to a hard drive” simply misstates the testimony. That something is *possible* does not mean it is *probable* or *easily* completed.

The defendant again misstates the record when he states, “there was ample evidence in this case that unidentified external drives were used to import child pornography to the hard drives in question.” Def Closing at pg. 20. The expert testified repeatedly, on both direct and cross-examination, that there was evidence that both the tablet and the laptop were used to view child pornography that was saved on an external drive. At no point in the expert’s testimony, did she say the evidence showed external drives were used to import child pornography onto either

device.¹² Moreover, the use of external drives (such as flash drives) to view child pornography is entirely consistent with the defendant's statement that he stored child pornography on flash drives.

Finally, the defendant faults the expert on two fronts. First, he faults the expert for not conducting an analysis, which would show nothing of significance. In particular, the defendant claims that the expert should have compared the files accessed from removable drives to the files accessed from the hard drives, implying that duplicates would show that the files originated from the removable drives. Def Closing at pgs. 20–21. The expert testified, and the government's summary exhibits show, that indeed, there were files with identical titles and sizes on both removable drives and the tablet. *See* Tr. 106:25–107:20 (“I didn’t do that for all of them. There were—the file names that—there was a couple that had file names on the external list and the jumplist.”); GEs 9-3, 9-11, and 9-14. Although comparing these two lists may be probative in a different case, it would reveal nothing of significance here, where the defendant said that he downloaded the same file multiple times and that he stored child pornography on removable drives. Thus, matches across those two lists is expected here.

Second, the defendant faults the expert for not locating evidence, which does not exist and would not be expected to exist if the crime occurred the way the defendant admitted it did. More specifically, the defendant asserts that there is some concern because the hash values of the files SA Abruzzese downloaded did not match the hash values of files in the expert's examination. The defendant also takes issue with the government not including hash values in

¹² The defendant did not cite any support in the record for the statement, and the closest the government has identified does not come close to saying what he claims: “it’s possible that . . . multiple external drives [were] used at different times throughout the lifetime of [the] tablet in order to upload files onto the C drive.” Tr. 110:4–8.

the summary exhibits. Def Closing at pgs. 10–13. On the first question, a hash match *should not* exist here because SA Abruzzese did not download the full files. Tr. 134:2–135:8. On the second question, the computer does not register the hash values for the records contained in the government’s summary exhibits. As such, it is impossible to present such evidence. *See* Tr. 135:10–16. Thus, an expert cannot be faulted for failing to find evidence that should not or could not exist.

Every piece of evidence that exists on the Asus tablet and Dell laptop is consistent with the defendant’s admissions. The evidence associated with Shareaza shows the defendant’s search terms, one of the files that SA Abruzzese downloaded is in the Shareaza\Incomplete folder along with multiple other child pornography videos, and additional child pornography was located in yet another folder associated with Shareaza. The tablet contained thumbnail files of child pornography, and not just any child pornography—child pornography matching SA Abruzzese’s downloads. Moreover, all of the evidence of file access and deletion also matches the defendant’s admissions. In addition, the government’s summary exhibits show matches across long, complicated file titles with identical size from Shareaza searches through file viewing all the way to file deletion, just like the defendant said.

As the expert testified, for all of this evidence to be located on the tablet and laptop in the way it is, it would require accessing or altering system files, database files, recycle bin files, thumb cache folders, and multiple Shareaza folders and subfolders. Moreover, all of this evidence would have needed to be fabricated or altered prior to SA Abruzzese interviewing the defendant. Frankly, it is difficult to comprehend how it is even theoretically possible that some unknown third person could fabricate evidence to match the defendant’s admissions prior to the defendant meeting with law enforcement. All of this is absurd. Obviously, the only reasonable

and believable explanation is that the evidence on the tablet and laptop exactly matches the defendant's statements because the defendant did exactly what he admitted: he used Shareaza to regularly search for and download child pornography.

III. The Defendant's As-Applied Proportionality Challenge Fails Because a Sentence of Five Years of Incarceration is Proportional to the Defendant's Conduct Given the Facts and Circumstances of this Case¹³

The defendant again raises the claim that the mandatory five years of incarceration that he must serve if he is convicted of receiving child pornography is cruel and usual as applied to him. *See* 18 U.S.C. § 2252(b)(1). The defendant's argument was meritless before trial. After the merits stage, however, the defendant's argument is not only meritless but also absurd because the United States has proven that the defendant was a frequent and long-time consumer of child pornography.

Punishment is "cruel and unusual" under the Eighth Amendment, when it is disproportionate to the crime for which it is imposed. *Graham v. Florida*, 560 U.S. 48, 59 (2010). Defendants may raise an Eighth Amendment challenge in two different ways. Under the "as applied" challenge, defendants contest a sentence as being disproportionate "given all the circumstances in a particular case." *Id.* The defendant may also raise a "categorical" challenge, which this defendant previously did and this Court rejected. "The Supreme Court has emphasized the limited scope of both types of proportionality challenges." *United States v. Cobler*, 748 F.3d 570, 575 (4th Cir. 2014).

The time has now come to convict the defendant of receiving child pornography. And with this conviction, now is also the time to deny the defendant's as applied challenge under the

¹³ We refer the Court to the United States' Response in Opposition to Defendant's Motion to Strike Mandatory Minimum Sentence (ECF No. 37) for its full briefing of this issue. In this section, the United States will address the defendant's main points.

Eighth Amendment. Put simply, overwhelming precedent establishes that a sentence of five years of imprisonment is proportional in the defendant's case.

In *Graham*, the Supreme Court explained that in the context of an as-applied challenge that the “narrow proportionality principle” of the Eighth Amendment “does not require strict proportionality between crime and sentence,” but “forbids only extreme sentences that are grossly disproportionate to the crime.” *Graham*, 560 U.S. at 59-60. The first step in this analysis is for a court to determine whether a “‘threshold comparison’ of the gravity of the offense and the severity of the sentence ‘leads to an inference of gross disproportionality.’” *United States v. Cobler*, 748 F.3d 570, 575 (4th Cir. 2014) (quoting *Harmelin v. Michigan*, 501 U.S. 957, 1005 (1991) (Kennedy, J., concurring)). Only if the defendant establishes a threshold inference of gross disproportionality, will courts then conduct an extended proportionality review, where a court is then required to compare the defendant's sentence to (1) sentences for other offenses in the same jurisdiction, and (2) sentences for similar offenses in other jurisdictions. *Id.* at 576. Here, the defendant cannot establish the threshold inference of gross disproportionality.

“The Supreme Court has identified a term-of-years sentence as being grossly disproportionate on only one occasion.” *Id.* In *Solem v. Helm*, 463 U.S. 277 (1983), a recidivist defendant challenged his sentence of life imprisonment without parole for passing a bad check in the amount of \$100. The Court found the defendant's sentence was grossly disproportionate because even though the check crime was “one of the most passive felonies a person could commit” the punishment was “the most severe non-capital sentence available.” *Solem*, 463 U.S. at 296-97. The *Solem* court noted that such proportionality challenges will rarely be successful, due to the “substantial deference” that courts owe to Congress. *Id.* at 289-90; *see also Hutto v.*

Davis, 454 U.S. 370, 374 (1982) (per curiam) (explaining that because there is “no clear way to make any constitutional distinction between one term of years and a shorter or longer term of years,” the “length of sentence actually imposed is purely a matter of legislative prerogative” and “successful challenges to proportionality of particular sentences should be exceedingly rare”).

Since *Solem*, both the Supreme Court and the Circuits have upheld every challenged sentence as proportionate under the Eighth Amendment. In *Harmelin*, the Supreme Court upheld a life sentence without parole for a first-time felon, who was convicted of possessing 672 grams of cocaine. *Harmelin*, 501 U.S. at 961, 996. And, in *Ewing v. California*, 538 U.S. 11 (2003), the Supreme Court upheld California’s three-strikes statute, which resulted in a defendant being sentenced to 25 years to life for stealing \$1,200 in merchandise. *Id.* at 28. The Supreme Court employing its reasoning in *Solem* explained that the theft crime was “certainly not ‘one of the most passive felonies a person could commit’” and, as such, a sentence of between 25 years and life imprisonment could be justified. *Ewing*, 538 U.S. at 28. So too here.

Here, the defendant’s crime is anything but passive. In this case, the defendant used the Shareaza program to repeatedly search for and receive child pornography since at least 2014. The defendant received videos and images detailing graphic sexual violence against young children, including a toddler. He also received and viewed the “Jason4” file on multiple occasions. *See* GEs 4-1, GE 4-5A, 9-15. This file details a young boy subjected to bondage while being sexually assaulted. For this reason, a sentence of five years of incarceration is proportionate to his crimes. *See Cobler*, 748 F.3d at 580 (applying this same analysis and upholding a sentence of 120 years of imprisonment, where a defendant possessed child pornography, which he downloaded and shared on the internet, and produced child pornography depicting his own sexual exploitation and abuse of a four-year-old child).

Additionally, every Circuit that has considered this question has refused to expand the proportionality principle and has upheld sentences in excess of five years of imprisonment for receipt of child pornography as consistent with the Eighth Amendment. *See, e.g., United States v. Gonzalez*, 731 Fed. Appx. 836 (11th Cir. 2018) (upholding a 1,200 month sentence for convictions of receipt of child pornography, two counts of possession of child pornography, and two counts of distribution of child pornography); *United States v. Niggeman*, 881 F.3d 976 (7th Cir. 2018) (upholding a sentence of 182 months in prison for a 67-year-old defendant convicted of receipt and possession of child pornography); *United States v. Reingold*, 731 F.3d 204, 216-17 (2d. Cir. 2013) (overruling the district court’s decision that a five-year mandatory minimum sentence for an “immature” defendant who distributed child pornography violated the Eighth Amendment); *United States v. Jamerson*, 536 Fed. Appx. 606, 610–11 (6th Cir. 2013) (upholding a five-year mandatory minimum sentence for receipt of child pornography); *United States v. Gray*, 455 Fed. Appx. 448 (5th Cir. 2011) (per curiam) (upholding a five-year sentence for convictions of receipt and possession of child pornography where the defendant claimed his poor health rendered it unlikely that he could serve the complete sentence).

The decisions in *Harmelin*, *Ewing*, *Cobler* and countless others reaffirm that that it will be an exceedingly rare case where a sentence for a term of years will violate the Eighth Amendment’s prohibition against cruel and unusual punishment. Moreover, as the above-cited cases demonstrate, there is a strong national consensus among the Circuits that have considered the issue that the mandatory minimum sentence for receipt of child pornography is proportionate. Here, a sentence of five years of imprisonment for actively searching for and

receiving child pornography, including videos detailing graphic violence against very young children, is proportionate and more than reasonable.

CONCLUSION

In order to acquit the defendant, this Court would have to believe the following fantastical series of events: (1) another person used Shareaza and the defendant's same exact search terms to obtain and download child pornography; (2) this other person, just like the defendant, viewed child pornography and then deleted the files after viewing; (3) this other person, just like the defendant, then began the cycle all over again by repeatedly searching for, downloading, and viewing many of the same videos over a four-year period; and (4) this other person decided to frame the defendant by placing the forensic evidence documenting their activity onto the defendant's tablet and laptop and/or decided to place all the evidence of their crimes on the defendant's tablet and laptop, where the defendant could locate evidence of their criminal activity. This is utter nonsense. The evidence admitted at trial allows for only one possible conclusion, which is that the defendant did exactly what he said: he repeatedly searched for, downloaded, and viewed child pornography from 2014 to 2018. For this reason, the United

